

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2002-157223**

2002-157223

(43)Date of publication of application : 31.05.2002

(51)Int.Cl.

G06F 15/00

G06F 17/30

G09C 1/00

H04L 9/08

H04L 9/32

(21)Application number : 2000-355635

(71)Applicant : HITACHI LTD

(22)Date of filing : 17.11.2000

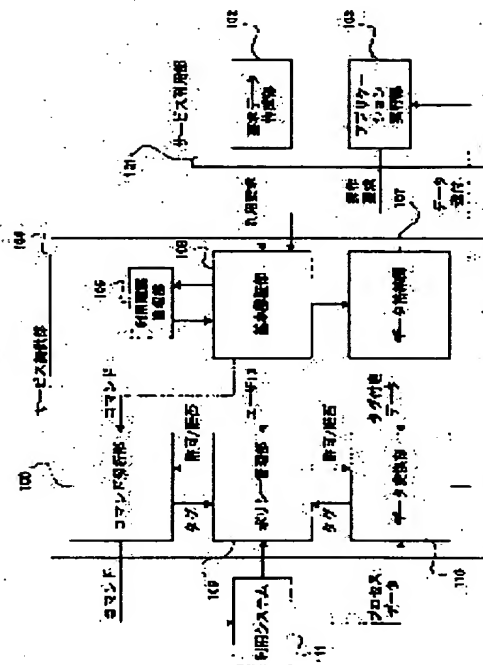
(72)Inventor : KATO HIROMITSU
FURUYA MASATOSHI
SEKOZAWA TERUJI
MIYAO TAKESHI

(54) SERVICE PROVIDING SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To dynamically select information to be transmitted/received according to the authority of a user, and to prevent the same operation from being received plural times by erroneous operation.

SOLUTION: In a request data preparing part 102, service utilization request data are prepared and sent to a basic authentication part 106. In the basic authentication part 106, the user is authenticated, and in respect to a legal user, a service utilization request is accepted. Requested data are retrieved by a data storage part 107 and dispatched to a data converting part 110. The data converting part 110 inquires whether tagged data can be provided to the user or not to a policy managing part 109. Corresponding to the user ID of the user, the tag and the state of a utilization system 111, the policy managing part 109 judges permission/refusal and the data converting part 110 converts data so that data permitted by the policy managing part 109 can be disclosed and refused data can be hidden, and provides the data to an application executing part 103.



LEGAL STATUS

[Date of request for examination]

29.01.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

*** NOTICES ***

JPO and INPIT are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1] A means to be the service provision system which performs information processing for offering predetermined service to a user, and to store the service information for offering said service, A means to receive requested data including the authentication child who attests the demand information which requires said contents of service, the user attribute which shows said user's description, and said user, A means to attest said user based on said user attribute and said authentication child, A means to determine said user's access propriety to the information included in said service information based on the result of said authentication, A means to retrieve the service information corresponding to said demand information from said accessible service information, The service provision system characterized by having a means to change said retrieved service information so that it may be adapted for said determined access propriety, and a means to show said changed service information.

[Claim 2] It is the service provision system characterized by inhibiting reception of the requested data inputted 2nd henceforth when the multiple input of the thing with said means same [the contents of said requested data] to receive is carried out in a service provision system according to claim 1.

[Claim 3] It is the service provision system characterized by receiving the requested data inputted 2nd henceforth [said] when checking carrying out a multiple input from said user when the multiple input of the thing with said means same [the contents of said requested data] to receive is carried out in a service provision system according to claim 2 is inputted.

[Claim 4] It is the service provision system characterized by showing the information which shows that it is a multiple input to said user when the multiple input of what has the contents of said requested data the same [said means to receive] is carried out in a service provision system according to claim 3. Therefore, the service provision system according to claim 1 to 2 characterized by having the function to restrict said available data attribute.

[Translation done.]

*** NOTICES ***

JPO and INPIT are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.*** shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the service provision system which performs protection of privacy, and unjust use prevention of contents by offering service suitable for what has a right especially about the service provision system which offers distribution of contents, and use of contents as service.

[0002]

[Description of the Prior Art] By development of the information communication technology represented by the Internet, through a network, contents, such as music and a game, are distributed or, generally the service which can perform inquiry for the balances and transfer is spreading from a cellular phone or the personal computer of a house like Internet banking. However, while corresponding to a service user's various needs, the need of fully taking into consideration the cure to the threat on an information security came out, because a service user becomes many and unspecified persons.

[0003] As shown in JP,2000-82039,A "a display-control information generation method and a computer", in order to offer the user interface according to each capacity as correspondence to various needs to the client terminal which has various capacity, there are some which generate display-control information, such as HTML, dynamically with reference to terminal attribute information.

[0004] Moreover, as a technique for securing an information security, JP,2000-19960,A is describing the "remote-operation approach" as follows. That is, if a user inputs a control signal in case a control signal is transmitted to a control unit from an operating station, the right of actuation is generated next time, and in a control unit side, a control signal and the signal which contains the right of actuation the right of actuation and this time next time will be enciphered with a common key, and it will transmit to an operating station. The right of actuation is memorized to an operating station next time. In a control unit side, the transmitted cipher is decrypted with a common key and the right of actuation is acquired the right of actuation, and next time a control signal and this time, it judges whether it is in agreement with the right of actuation which has registered the right of actuation into the control unit side this time, and when in agreement, a control signal is sent to a control equipment. The right of actuation is registered into a control unit side next time.

[0005]

[Problem(s) to be Solved by the Invention] There are the following problems in this conventional approach. That is, although the contents offered based on the terminal attribute information transmitted from a client terminal are dynamically generated in case contents are offered about JP,2000-82039,A, it is not considered whether there is any authority for the user who is perusing using a terminal to peruse the contents. In the case of that in which contents contain important extra sensitive information, a thing to be protected [of privacy], the thing with which only a member is limited and provided, it is necessary to perform generation and distribution for contents in consideration of the authority of the contents user who becomes an offer partner.

[0006] moreover, JP,2000-19960,A -- being related -- from an operating station -- mistaking -- multiple times -- when the same actuation is performed, a control unit recognizes it as the just

control signal having been sent two or more times, may repeat the same control and may be performed. For example, there was a problem of transferring a large sum beyond the need, without detecting it, when this technique was applied to Internet banking, and multiple-times transmission has been carried out accidentally [signal / transfer actuation].

[0007] The purpose of this invention is to offer the service provision system which selects dynamically the information offered in accordance with a user's authority, and the information to receive.

[0008] Other purposes of this invention are to offer the service provision system which is not without a check of a user a multiple-times receptionist, also when multiple-times transmission of the same control signal has been carried out accidentally at service utilization time.

[0009]

[Means for Solving the Problem] A means for this invention to be a service provision system which performs information processing for offering predetermined service to a user, and to store two or more service information for offering said service; A means to receive requested data including the authentication child who attests the demand information which requires said contents of service, the user attribute which shows said user's description, and said user, A means to attest said user based on said user attribute and said authentication child, A means to determine said user's access propriety to the information included in said service information based on the result of said authentication, It has a means to retrieve the service information corresponding to said demand information from said accessible service information, a means to change said retrieved service information so that it may be adapted for said determined access propriety, and a means to show said changed service information. In addition, a display of accessible information is enabled and it includes inhibiting presenting of the information which cannot be accessed in conversion.

[0010] Moreover, with another gestalt of this invention, it is characterized by inhibiting reception of the same requested data.

[0011] The others and following service provision system is also contained in this invention. The service provision system which has the requested data creation section which attaches a user attribute and an authentication child and creates a request, a user attribute and the basic authentication section which performs user authentication from an authentication child, the policy Management Department which specifies an accessible data attribute, the data storage section which takes out the data demanded based on a request, and the data-conversion section with which reconstruct data according to the data attribute specified by the policy Management Department, and a user is provided.

[0012] Moreover, the service provision system have a confirmation-of-receipt value, the application activation section which attach a user attribute and an authentication child to the actuation demand characterized according to the data attribute, and transmit to it, a user attribute and the basic authentication section which perform user authentication from an authentication child, the use hysteresis Management Department which confirm whether a confirmation-of-receipt value is a thing [finishing / reception], the policy Management Department which specify an accessible data attribute, and the command analysis section which analyze in an actuation demand and operate in a use system based on decision of the policy Management Department.

[0013] Furthermore, in each above-mentioned service provision system, the policy Management Department has the function in which a user attribute restricts an available data attribute, and the function to restrict an available data attribute according to the condition of a use system.

[0014] Furthermore, the service provision system by which the basic authentication section has the function which updates a confirmation-of-receipt value, and the function which enciphers a confirmation-of-receipt value in the form which only a user can decrypt is also contained in this invention.

[0015] Furthermore, the service provision system which has the function to check that the application activation section has received the confirmation-of-receipt value answered from the basic authentication section, and the function to decrypt a confirmation-of-receipt value and to save an actuation demand next time for transmission is also contained in this invention.

[0016]

[Embodiment of the Invention] Hereafter, the gestalt of operation of this invention is explained using a drawing. As one gestalt of operation of this invention, the block diagram at the time of applying this invention to a plant SCS is shown in drawing 1. To drawing 1, a means by which the service use section 101 receives information from the service provision section 104, and a means by which the service use section 101 operates it to the use system 111 are indicated.

[0017] The service use section 101 consists of the requested data creation section 102 and the application activation section 103. The requested data creation section 102 sends a demand of a user to the service provision section 106 with user ID, a password, etc. The application activation section 103 peruses the data passed from the service provision section 106, or operates it to the use system 111.

[0018] The service provision section 104 consists of the use hysteresis Management Department 105, the basic authentication section 106, the data storage section 107, the policy Management Department 109, the data-conversion section 110, and the command analysis section 108. The use hysteresis Management Department 105 manages a user's use hysteresis. The basic authentication section 106 attests a user. The data storage section 107 stores data and searches required data according to a demand. The policy Management Department 109 judges [to which data use is permitted / or or] whether refusal is carried out. The data-conversion section 110 changes data into a form with an available user. The command analysis section 108 analyzes the actuation command to the use system 111 sent from the service use section 101.

[0019] First, the service use section 101 explains the processing flow which receives information according to drawing 2 from the service provision section 104. The service use section 101 specifies the data I want you to give and provide with authentication information in the requested data creation section 102 (step 201), and requires them of the service provision section 104 (step 202). A user attribute and an authentication child check correctly whether it is ***** with relation in the basic authentication section 106, and a user is attested (step 203). If a user is attested, the basic authentication section 106 will perform the retrieval demand of data to the data storage section 107 (step 204). The data storage section 107 searches the demanded data (step 205). Here, each data element is characterized with the tag as a data attribute by the data stored in the data storage section 107. The data-conversion section 110 reads the tag of the searched data with a tag (step 206), and asks the policy Management Department 109 whether an applicable user may be provided with each data with a tag (step 207). The policy Management Department 109 judges authorization and refusal of data offer based on the user ID and the tag which the basic authentication section 106 attested (step 208). Based on the judgment result of the policy Management Department 109, the data-conversion section 110 indicates the data to permit, and conceals the data to refuse (step 209). The data-conversion section 110 performs cryptocommunication, in order to provide a user with the created data (step 210). The existing technique, such as SSL, can be used as the cryptocommunication approach. If the data which used in the pair the public key which can be opened to everybody in a public key cryptosystem, and the private key which must be made secret in the individual here, and were enciphered with the public key are not a private key used as a pair, they have the property in which it cannot decode to the original data. Only the attested user can be provided with data by enciphering and passing the cryptographic key used for cryptocommunication with a public key using this property. A user's public key guarantees the owner of a key, when the independent organization which can trust it publishes a digital certificate.

[0020] The concrete image for every processing step is shown below. The example of the requested data creation section 102 is shown in drawing 3. In drawing 3, user ID 301 is chosen as a user attribute, and requested data 304 (here, they are "a pump and a bulb") is chosen from the service list 303 wishing use as data I want you to offer. It is enciphered with the password, and a user's private key has the term which enters a password 302, in order to decrypt this. The decrypted private key is used for performing a digital signature to user ID 301 and requested data 304. By pushing the "log in" carbon button 305, the certificate 402 of the public key which is user ID 301, the set of requested data 304 and the digital signature 401 of this, the private key used for the signature, and a pair like drawing 4 is transmitted to the service provision section 104, and it requires of the service provision section 104 (step 202). Since user authentication can be performed by verifying a digital signature

401, with the gestalt of this operation, a digital signature 401 is used as an authentication child. In canceling, it pushes "cancellation" carbon button 306.

[0021] In the basic authentication section 106, a certificate 402 is verified and a right public key is acquired. A digital signature 401 is checked using a public key, and a user is attested (step 203). When it is able to be checked that he is a just user, the basic authentication section 106 passes user ID for the retrieval demand of the data demanded from the data storage section 107 to delivery (step 204) and the policy Management Department 109. The data which correspond according to the passed data demand are searched with the data storage section (step 205). "The pump and the bulb" are passed as requested data 304, and the file relevant to the supervisory-control screen of a pump and a bulb is searched with this example. The example of the searched file is shown in drawing 5. The data in a file are characterized with the tag.

[0022] Here, $\langle x \rangle y \langle /x \rangle$ characterizes and Data y are characterized with Tag x. The data file of this format has a standard description language called XML (eXtensible Markup Language). In the case of drawing 5, pump tag 501a connoted the components which constitute the supervisory-control screen of a pump, and has generalized stop tag 501d which performs watch tag 501b which makes a monitor screen, start tag 501c which performs pump starting control, and pump halt control. Similarly, valve tag 501e connoted the components which constitute the supervisory-control screen of a bulb, and has generalized watch tag 501f which makes a monitor screen, open tag 501g which performs control which opens a bulb, and close tag 501h which performs control which closes a bulb. By this example, the screen configuration program 502 for performing supervisory control is placed as data surrounded with the tag 501.

[0023] The above-mentioned data file with a tag is passed to the data-conversion section 110, and is taken as the master data for constituting the data shown to the service use section 101. In the data-conversion section 110, the data to which the tag 501 was read (step 206) and the corresponding tag 501 was attached are asked [whether you may provide for the service use section 101, and] to the policy Management Department 109 (step 207). At the policy Management Department 109, authorization and refusal about offer of data are judged from the user ID 301 passed from the basic authentication section 106, and the tag 501 passed from the data-conversion section 110 (step 208).

[0024] The matrix for performing this decision is shown in drawing 6. In drawing 6, it is user ID 301 a-c and the matrix of tag 501 a-h, and Ox within a matrix is expressing authorization and refusal. For example, it is refused for it to offer a halt control screen that user ID 301 offers the monitor screen of a pump to the user of user A, although the permission is granted. The conditional statement in a matrix describes the conditions for permitting information offer. In conditional-statement 601a of drawing 6, it has set up with "IF power-source =ON" as conditions for user ID 301 to offer a pump monitor screen to the user of user B. This is restricted when the power source of a pump is ON, and it means offering a pump monitor screen. Similarly as conditions for user ID 301 to offer a pump starting screen to the user of user A Conditional-statement 601b describes as "IF t>9:00 and t>17:00" that time of day t is from 9:00 to 17:00. As conditions for user ID 301 to provide the user of user B with a pump halt screen, conditional-statement 601c has described that the rotational frequency of a pump is less than 10000 as "IF rotational frequency <10000."

[0025] In drawing 3, the user of user B has advanced the service use demand of "a pump and a bulb", and user ID 301 presupposes that the data file with a tag of drawing 5 was searched corresponding to this. In the data-conversion section 110, the file 701 from which it cooperated with the policy Management Department 109, and the format of drawing 7 was changed is formed. The power source of a pump is ON, when the rotational frequency of a pump is less than 10000, to user B, presentation of a pump monitor screen, a pump halt screen, a bulb monitor screen, and a bulb close screen is permitted, and drawing 7 is made into the HTML file which is the data format at the time of offering information by Web. The service user who received the data of drawing 7 shows the image perused by the web browser to drawing 8. On a screen, the pump monitor screen 801, the pump halt screen 802, the bulb monitor screen 803, and the bulb close screen 804 are displayed. On the other hand, the power source of a pump is off, and since offer of the pump monitor screen 801 and the pump halt screen 802 is refused when a pump rotational frequency is 10000 or less, the screen which can peruse the service use section 101 turns into the bulb monitor screen 803 and the

"bulb close screen 804 like drawing 9 .

[0026] As mentioned above, although the case where a supervisory-control screen was perused was described, the same processing is possible also when perusing a common document. Secret papers 1001 like drawing 10 as a data file with a tag are searched and carried out from the data storage section 107 to the perusal demand of secret papers. Secret papers 1001 are managed by secret tag 501i, and define s1, s2, and s3 tag here according to security level, respectively. For example, ***** level and s2 tag 501k can define management level and s3 tag 501L as extra sensitive information of officer level, and s1 tag 501j can constitute secret papers 1001. The data-conversion section 110 reconfigures this data with a tag, and the data which can be offered by inquiry of authorization and refusal to the policy Management Department 109.

[0027] At the policy Management Department 109, authorization and refusal are judged using the matrix shown in drawing 11 . The perusal possibility of and user ID 301 show that all data can peruse the user of user C except the officer data with which, as for the user of user B, s3 tag 501L attachment of the perusal possibility of and user ID 301 was done only for the ***** data with which, as for drawing 11 , s1 tag 501i attachment of user ID 301 was done, as for the user of user A. User ID 301 changes into a "****" mark the data surrounded with s3 tag to the user who is user B, and makes the data-conversion section 110 perusal impossible here. The example of the changed HTML file is shown in drawing 12 . The HTML file offered from the data-conversion section 110 is passed to a service user's application activation section 103 by the cryptocommunication of step 210 described previously.

[0028] This example of a screen display is shown in drawing 13 . If there is no private key for decrypting the cryptographic key used for cryptocommunication even when a third person intercepts the data which flow a network top, it will become possible to prevent the display of the screen of drawing 10 .

[0029] With the gestalt of this operation, if a user changes or the condition of a use system changes, the description will be in the place where the information to offer also changes, and security and privacy protection will be realized.

[0030] Next, how the service use section 101 operates it safely to the use system 111 is explained using the processing flow of drawing 14 . By pushing the pump earth switch 805 in drawing 8 as an example, the case where a pump PAUSE command is transmitted to the service provision section 104 is considered.

[0031] When the pump earth switch 805 is pushed, the application activation section 103 creates the set of the value and command which have taken the synchronization in the service provision section 104 and the service use section 101 as one data (step 1401). Time of day, a counter, etc. can be considered as data which have taken the synchronization.

[0032] As shown in drawing 15 , let a command 1501 be data with a tag. It is shown by command tag 501m that it is a command, and target tag 501n shows that it is the command which suspends a pump by the transmission place of a command, pump tag 501a, and stop tag 501c. "ad%f38 wh!f74" is the control signal 1502 which should actually be transmitted to the use system 111, and is a special value depending on the use system 111.

[0033] Next, it is enciphered with user ID 301 and a counter 1503 using the cryptographic key generated at random (step 1402), and the command 1501 as data with a tag forms the code data 1504. A cryptographic key is enciphered with the public key of the service provision section (step 1403). The code data 1504 and the enciphered cryptographic key 1505 are signed with the private key of the service use section 101 (step 1404). In the application activation section 103, the digital certificate 1507 for verifying the code data 1504, the enciphered cryptographic key 1505, the signature data 1506, and a signature is made a set, and it transmits to the basic authentication section 106 (step 1405).

[0034] In the basic authentication section 106, a digital certificate 1507 is verified, a user's public key is acquired (step 1406) and the signature data 1503 are verified with a public key (step 1407). The basic authentication section 106 decrypts the cryptographic key 1505 enciphered using the private key of the service provision section 104, and obtains a cryptographic key (step 1408). The code data 1504 are decrypted using this cryptographic key, and a counter 1503 and a command 1501 are

obtained (step 1409). The basic authentication section 106 asks the use hysteresis Management Department 105 a counter 1503, and it confirms whether be a thing [finishing / reception / already] (step 1410). If it is reception ending, a command 1501 will be refused (step 1411), if it is not reception ending, this user's counter 1503 registered into the use hysteresis Management Department 105 will be updated to the newest thing (step 1412), and a command 1501 will be passed to the command analysis section (step 1413). For example, when a user's counter 1503 saved in the application activation section 103 is n , the value of a counter 1503 is attached as $n+1$. When the transmitted counter 1503 is below n , it judges that transmit data is already reception ending, and dismisses. If the transmitted counter 1503 is $n+1$, a command 1501 will be attested and the registration value of the use hysteresis Management Department 105 will be updated to $n+1$. It is enciphered with a user's public key and the new counter 1503 is answered by the service use section 101 (step 1414). In the application activation section 103, when the enciphered counter 1503 is received, a confirmation-of-receipt screen is displayed (step 1415), a counter 1503 is decrypted with a user's private key, and it is saved for the next command transmission (step 1416).

[0035] With the gestalt of this operation, the description is in the place which has prevented reception of the multiple times of the same command using the value which synchronizes in the service use section 101 and the service provision section 104. In the case of the system using the Internet, there is an unlawful access technique of the resending attack which transmits the data intercepted in the middle of the network as it is, and this is prevented.

[0036] Moreover, also when the multiple-times carbon button has been pushed accidentally, two or more same commands cannot be received and an operation mistake can be prevented. Moreover, it can also be checked that the transmitted command has been certainly sent to the use system 111.

[0037] The processing flow in the command analysis section 108 is shown in drawing 16. The command analysis section 108 analyzes the tag 501 of a command 1501 (step 1601), and asks the policy Management Department 109 use authorization of a tag 501 (step 1602). At the policy Management Department 109, authorization and refusal are judged based on the condition of user ID 301, a tag 501, and the use system 111 (step 1603). In refusal, the purport user who is refusal is notified (step 1604), and the control signal 1502 which was surrounded with the tag in authorization is transmitted to the use system 111 (step 1605).

[0038] With the gestalt of this operation, also when data formats differ for every device of a controlled system (for example, pump) by surrounding a control signal 1502 with a tag 501, and transmitting (A company is X method and B company is Y method etc.), if the controlled system itself is the same, the description is in the place which can perform an access control with the same method.

[0039]

[Effect of the Invention] As stated above, according to this invention, the contents itself offered according to the condition of a user or a use system can be changed, and security and privacy protection can be realized. Moreover, a resending attack and an operation mistake can be prevented. Moreover, also when data formats differ for every device of a controlled system, the description is in the place which can apply an access control with the same method by a controlled system being characterized with the same tag.

[Translation done.]

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2002-157223

(P2002-157223A)

(43)公開日 平成14年5月31日(2002.5.31)

(51)Int.Cl. ⁷	識別記号	F I	テーマコード(参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 B 5 B 0 7 5
17/30	1 1 0	17/30	1 1 0 F 5 B 0 8 5
	1 2 0		1 2 0 B 5 J 1 0 4
			1 2 0 A
	2 4 0		2 4 0 C

審査請求 未請求 請求項の数 4 O L (全 11 頁) 最終頁に続く

(21)出願番号 特願2000-355635(P2000-355635)

(22)出願日 平成12年11月17日(2000.11.17)

(71)出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72)発明者 加藤 博光

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(72)発明者 古谷 雅年

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(74)代理人 100075096

弁理士 作田 康夫

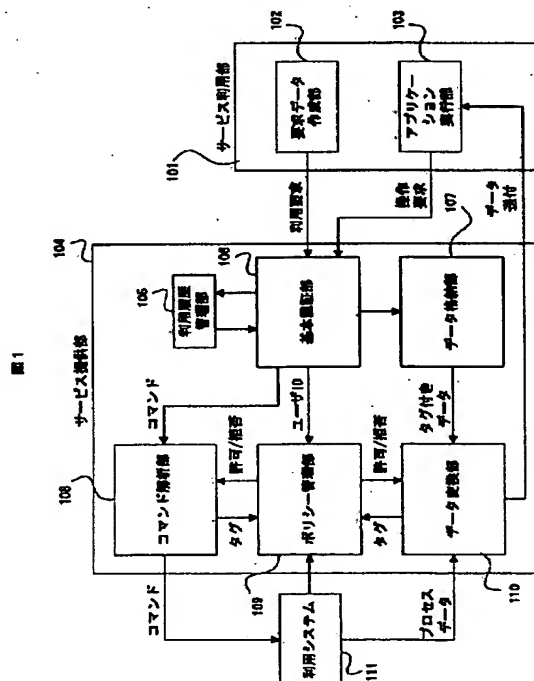
最終頁に続く

(54)【発明の名称】 サービス提供システム

(57)【要約】

【課題】利用者の権限に沿って送受信する情報を動的に取捨選択し、かつ、誤操作による同じ操作の複数回受信を防止する。

【解決手段】要求データ作成部102においてサービス利用要求データを作成し、基本認証部106に送る。基本認証部106では利用者を認証し、正当な利用者に対してサービス利用要求を受け付ける。要求されたデータをデータ格納部107は検索し、データ変換部110に渡す。データ変換部110はタグ付けされたデータを利用者に提供して良いかポリシー管理部109に問い合わせる。ポリシー管理部109は、利用者のユーザIDとタグ、および利用システム111の状態によって許可・拒否の判断を下し、データ変換部110はポリシー管理部109によって許可されたデータを開示し、拒否されたデータは隠蔽するようにデータを変換し、アプリケーション実行部103にデータを提供する。



1

【特許請求の範囲】

【請求項1】利用者に対して所定のサービスを提供するための情報処理を実行するサービス提供システムであって、

前記サービスを提供するためのサービス情報を格納する手段と、

前記サービス内容を要求する要求情報、前記利用者の特徴を示すユーザ属性および前記利用者を認証する認証子を含む要求データを受付ける手段と、

前記ユーザ属性および前記認証子に基づいて、前記利用者を認証する手段と、

前記認証の結果に基づいて、前記サービス情報に含まれる情報に対する前記利用者のアクセス可否を決定する手段と、

前記要求情報に対応するサービス情報を、前記アクセス可能なサービス情報から検索する手段と、

検索された前記サービス情報を、決定された前記アクセス可否に適用するよう変換する手段と、

変換された前記サービス情報を提示する手段とを有することを特徴とするサービス提供システム。

【請求項2】請求項1に記載のサービス提供システムにおいて、

前記受付ける手段は、前記要求データの内容の同じものが複数入力された場合には、2回目以降に入力された要求データの受信を抑制することを特徴とするサービス提供システム。

【請求項3】請求項2に記載のサービス提供システムにおいて、

前記受付ける手段は、前記要求データの内容の同じものが複数入力された場合、前記利用者から複数入力することを確認することが入力された場合は、前記2回目以降に入力された要求データを受信することを特徴とするサービス提供システム。

【請求項4】請求項3に記載のサービス提供システムにおいて、

前記受付ける手段は、前記要求データの内容の同じものが複数入力された場合には、前記利用者に対して、複数入力であることを示す情報を提示することを特徴とするサービス提供システム。よって利用可能な前記データ属性を制限する機能を有することを特徴とする請求項1乃至2に記載のサービス提供システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はコンテンツの配信およびコンテンツの利用をサービスとして提供するサービス提供システムに関し、特に、権利のあるものに適切にサービスを提供することでプライバシーの保護、コンテンツの不正利用防止を行なうサービス提供システムに関する。

【0002】

2

【従来の技術】インターネットに代表される情報通信技術の発展によって、ネットワークを介して音楽やゲームなどのコンテンツを配信したり、インターネットバンキングのように携帯電話や自宅のパソコンから残高照会や振込みを行なえるサービスが一般に普及してきている。ところが、サービス利用者が不特定多数となることで、サービス利用者の多様なニーズに対応するとともに、情報セキュリティ上の脅威への対策を十分に考慮していく必要がでてきた。

【0003】多様なニーズへの対応として、例えば特開2000-82039号「表示制御情報生成方法およびコンピュータ」に示されるように、様々な能力を有するクライアント端末に対して、それぞれの能力に応じたユーザインターフェースを提供するために、端末属性情報を参照してHTML等の表示制御情報を動的に生成するものがある。

【0004】また情報セキュリティを確保するための技術として、特開2000-19960号では「遠隔操作方法」を次のように記している。すなわち、操作端末から制御装置に制御信号を送信する際に、ユーザが制御信号を入力すると、次回操作権を発生し、制御装置側では制御信号と次回操作権と今回操作権を含む信号を共通鍵で暗号化し、操作端末に転送する。次回操作権は操作端末に記憶する。制御装置側では転送された暗号文を共通鍵で復号化し、制御信号と今回操作権と次回操作権とを取得し、今回操作権が制御装置側に登録してある操作権と一致するかを判定し、一致する場合は制御機器に制御信号を送る。次回操作権は制御装置側に登録される。

【0005】

【発明が解決しようとする課題】かかる従来方法においては次のような問題がある。すなわち、特開2000-82039号に関しては、コンテンツを提供する際には、クライアント端末から送信される端末属性情報に基づいて提供するコンテンツを動的に生成するが、端末を利用して閲覧している利用者がそのコンテンツを閲覧する権限があるかどうか加味されない。コンテンツが重要な機密情報を含んでいるもの、プライバシーの保護が必要なもの、会員のみ限定して提供するもの等の場合には、提供相手となるコンテンツ利用者の権限を考慮してコンテンツを生成・配信を行なう必要がある。

【0006】また、特開2000-19960号に関しては、操作端末から誤って複数回同じ操作を行なった場合、制御装置は正当な制御信号が複数回送られてきたと認識して、同じ制御を繰り返し実行してしまう可能性がある。例えば、インターネットバンキングに本手法を適用すると、振込み操作信号を誤って複数回送信してしまった場合には、それを検知することなく、必要以上に多額の振込みをしてしまうという問題があった。

【0007】本発明の目的は、利用者の権限に沿って提供する情報、受け取る情報を動的に取捨選択するサービ

50

3

ス提供システムを提供することにある。

【0008】本発明の他の目的は、サービス利用時に誤って同じ制御信号を複数回送信してしまった場合にも、利用者の確認無しには複数回受け付けられないサービス提供システムを提供することにある。

【0009】

【課題を解決するための手段】本発明は、利用者に対して所定のサービスを提供するための情報処理を実行するサービス提供システムであって、前記サービスを提供するための複数のサービス情報を格納する手段と、前記サービス内容を要求する要求情報、前記利用者の特徴を示すユーザ属性および前記利用者を認証する認証子を含む要求データを受付ける手段と、前記ユーザ属性および前記認証子に基づいて、前記利用者を認証する手段と、前記認証の結果に基づいて、前記サービス情報に含まれる情報に対する前記利用者のアクセス可否を決定する手段と、前記要求情報に対応するサービス情報を、前記アクセス可能なサービス情報から検索する手段と、検索された前記サービス情報を、決定された前記アクセス可否に20 適応するよう変換する手段と、変換された前記サービス情報を提示する手段とを有する。なお、変換には、アクセス可能な情報を表示可能とし、アクセス不可能な情報の表示を抑止することを含む。

【0010】また、本発明の別の形態では、同じ要求データの受信を抑止することを特徴とする。

【0011】他、以下のサービス提供システムも本発明に含まれる。ユーザ属性と認証子を添付してリクエストを作成する要求データ作成部と、ユーザ属性と認証子からユーザ認証を行なう基本認証部と、アクセス可能なデータ属性を指定するポリシー管理部と、リクエストに基づいて要求されるデータを取り出すデータ格納部と、ポリシー管理部によって指定されたデータ属性に従ってデータを再構築してユーザに提供するデータ変換部を有するサービス提供システム。

【0012】また、送達確認値と、データ属性によって特徴付けられた操作要求に、ユーザ属性と認証子を添付して送信するアプリケーション実行部と、ユーザ属性と認証子からユーザ認証を行なう基本認証部と、送達確認値が受信済みのものでないかチェックを行なう利用履歴管理部と、アクセス可能なデータ属性を指定するポリシー管理部と、操作要求を解析しポリシー管理部の判断に基づいて利用システムを操作するコマンド解析部を有するサービス提供システム。

【0013】さらに、上記のサービス提供システムそれぞれにおいて、ポリシー管理部が、ユーザ属性によって利用可能なデータ属性を制限する機能と、利用システムの状態によって利用可能なデータ属性を制限する機能を有する。

【0014】さらに、基本認証部が、送達確認値を更新する機能と、送達確認値を利用者のみが復号化できる形

4

で暗号化する機能を有するサービス提供システムも本発明に含まれる。

【0015】さらに、アプリケーション実行部が、基本認証部から返信された送達確認値を受信したことを確認する機能と、送達確認値を復号化して操作要求を次回送信のために保存する機能を有するサービス提供システムも本発明に含まれる。

【0016】

【発明の実施の形態】以下、本発明の実施の形態を、図面を用いて説明する。本発明の実施の一形態として、プラント監視制御システムに本発明を適用した場合のブロック図を図1に示す。図1にはサービス利用部101がサービス提供部104から情報を入手する手段と、サービス利用部101が利用システム111に対して操作を行なう手段とを記載している。

【0017】サービス利用部101は、要求データ作成部102とアプリケーション実行部103からなる。要求データ作成部102は、利用者の要求をユーザID、パスワード等とともにサービス提供部106に送る。アプリケーション実行部103はサービス提供部106から渡されたデータを閲覧したり、利用システム111に対して操作を行なったりするものである。

【0018】サービス提供部104は、利用履歴管理部105、基本認証部106、データ格納部107、ポリシー管理部109、データ変換部110、コマンド解析部108からなる。利用履歴管理部105は利用者の利用履歴を管理する。基本認証部106は利用者の認証を行なう。データ格納部107はデータを格納しておき要求に応じて必要なデータを検索する。ポリシー管理部109はデータ利用を許可するか拒否するかを判断する。データ変換部110は利用者が利用可能な形にデータを変換する。コマンド解析部108は、サービス利用部101から送られた利用システム111に対する操作コマンドを解析する。

【0019】まず、サービス利用部101がサービス提供部104から情報を入手する処理フローを図2に従って説明する。サービス利用部101は、要求データ作成部102において認証情報を付与して提供して欲しいデータを指定し（ステップ201）、サービス提供部104に要求する（ステップ202）。基本認証部106でユーザ属性と認証子が正確に関連付いているかを確認し利用者の認証を行なう（ステップ203）。利用者が認証されると、基本認証部106はデータ格納部107に対してデータの検索要求を行なう（ステップ204）。データ格納部107は要求されたデータを検索する（ステップ205）。ここで、データ格納部107に格納されているデータは各データ要素を、データ属性としてタグによって特徴付けている。データ変換部110は、検索されたタグ付きデータのタグを読み取り（ステップ206）、各々のタグ付きデータを該当利用者に提供して

5

よいかどうかをポリシー管理部109に問い合わせる(ステップ207)。ポリシー管理部109は基本認証部106が認証したユーザIDとタグをもとにデータ提供の許可・拒否を判定する(ステップ208)。データ変換部110はポリシー管理部109の判定結果に基づき、許可するデータは開示し、拒否するデータは隠蔽する(ステップ209)。データ変換部110は、作成したデータを利用者に提供するために暗号通信を行なう(ステップ210)。暗号通信方法としてはSSL等の既存の手法を用いることができる。ここで、公開鍵暗号方式では、皆に公開できる公開鍵と、個人で秘密にしていなければならない秘密鍵をペアで用い、公開鍵で暗号化したデータは、対となる秘密鍵でないと元のデータに復号できないという性質がある。この性質を利用して、暗号通信に用いる暗号鍵を公開鍵で暗号化して渡すことによって、認証された利用者のみにデータを提供することができる。利用者の公開鍵は、信頼できる第三者機関が電子証明書を発行することによって鍵の持ち主を保証する。

【0020】各処理ステップ毎の具体的なイメージを以下に示す。要求データ作成部102の具体例を図3に示す。図3では、ユーザ属性としてユーザID301、提供して欲しいデータとして利用希望サービスリスト303から要求データ304(ここでは「ポンプとバルブ」)を選択している。利用者の秘密鍵はパスワードによって暗号化されており、これを復号化するためにパスワード302を入力する項がある。復号化された秘密鍵は、ユーザID301と要求データ304に対してデジタル署名を行なうことに用いる。「ログイン」ボタン305を押すことにより、図4のように、ユーザID301と要求データ304のセット、これのデジタル署名401と、署名に用いた秘密鍵と対になっている公開鍵の証明書402をサービス提供部104に送信し、サービス提供部104に要求する(ステップ202)。デジタル署名401を検証することによってユーザ認証を行なうことができるので、本実施の形態では認証子としてデジタル署名401を用いる。キャンセルする場合には「キャンセル」ボタン306を押す。

【0021】基本認証部106では証明書402を検証し、正しい公開鍵を取得する。公開鍵を用いてデジタル署名401をチェックして利用者の認証を行なう(ステップ203)。正当な利用者であることが確認できた場合には、基本認証部106はデータ格納部107に対して要求されたデータの検索要求を渡し(ステップ204)、ポリシー管理部109に対してユーザIDを渡す。データ格納部では渡されたデータ要求に従って該当するデータを検索する(ステップ205)。本実施例では要求データ304として「ポンプとバルブ」を渡しており、ポンプとバルブの監視制御画面に関連するファイルを検索する。検索されたファイルの具体例を図5に示

6

す。ファイル内のデータはタグによって特徴付けられている。

【0022】ここで、 $\langle x \rangle y \langle /x \rangle$ はデータyはタグxで特徴付けられている。この形式のデータファイルはXML(Extensible Markup Language)という標準的な記述言語がある。図5の場合、pumpタグ501aはポンプの監視制御画面を構成する部品を内包し、監視画面を作るwatchタグ501b、ポンプ起動制御を行なうstartタグ501c、ポンプ停止制御を行なうstopタグ501dを統括している。同様にして、valveタグ501eはバルブの監視制御画面を構成する部品を内包し、監視画面を作るwatchタグ501f、バルブを開く制御を行なうopentag501g、バルブを閉じる制御を行なうclosetag501hを統括している。タグ501で囲まれたデータとして本実施例では監視制御を行なうための画面構成プログラム502を置いている。

【0023】上記のタグ付きデータファイルはデータ変換部110に渡され、サービス利用部101に提示するデータを構成するための基本データとする。データ変換部110ではタグ501を読み取り(ステップ206)、該当するタグ501の付いたデータをサービス利用部101に提供してよいかどうかポリシー管理部109に問い合わせる(ステップ207)。ポリシー管理部109では、基本認証部106から渡されたユーザID301と、データ変換部110から渡されたタグ501からデータの提供に関する許可・拒否の判断を行なう(ステップ208)。

【0024】この判断を行なうためのマトリックスを図6に示す。図6ではユーザID301a~cとタグ501a~hのマトリックスとなっており、マトリックス内のO×によって許可と拒否を表現している。例えば、ユーザID301aがuser Aのユーザに対してポンプの監視画面を提供することは許可されているが、停止制御画面を提供することは拒否される。マトリックス中の条件文は情報提供を許可するための条件を記す。図6の条件文601aでは、ユーザID301aがuser Bのユーザに対してポンプ監視画面を提供するための条件として「IF 電源=ON」と設定している。これは、ポンプの電源がオンの場合に限り、ポンプ監視画面を提供することを表す。同様にして、ユーザID301aがuser Aのユーザに対してポンプ起動画面を提供するための条件として、時刻tが9:00から17:00までであることを、条件文601bにて「IF t>9:00 and t<17:00」として記述し、ユーザID301aがuser Bのユーザにポンプ停止画面を提供するための条件として、ポンプの回転数が10000未満であることを、条件文601cにて「IF 回転数<10000」として記述している。

【0025】図3ではユーザID301aがuser Bのユー

7

ザが「ポンプとバルブ」のサービス利用要求を出しており、これに対応して図5のタグ付きデータファイルが検索されたとする。データ変換部110では、ポリシー管理部109と連携して図7の形式の変換されたファイル701を形成する。ポンプの電源がオンで、ポンプの回転数が10000未満の場合にはuser Bに対して、ポンプ監視画面、ポンプ停止画面、バルブ監視画面、バルブ閉画面の提示が許可されており、図7はWebで情報を提供する際のデータ形式であるHTMLファイルにしたものである。図7のデータを受信したサービス利用者がWebブラウザで閲覧したイメージを図8に示す。画面上には、ポンプ監視画面801、ポンプ停止画面802、バルブ監視画面803、バルブ閉画面804が表示される。一方、ポンプの電源がオフで、ポンプ回転数が10000以下の場合には、ポンプ監視画面801、ポンプ停止画面802の提供が拒否されるので、サービス利用部101が閲覧できる画面は図9のようにバルブ監視画面803およびバルブ閉画面804になる。

【0026】以上、監視制御画面を閲覧する場合について述べたが、一般の文書を閲覧する場合にも同様な処理が可能である。機密文書の閲覧要求に対して、データ格納部107からタグ付きデータファイルとして図10のような機密文書1001を検索したとする。ここで機密文書1001はsecretタグ501iで管理され、セキュリティレベルに応じてs1、s2、s3タグをそれぞれ定義する。例えば、s1タグ501jは社内秘レベル、s2タグ501kは幹部レベル、s3タグ501Lは役員レベルの機密情報として定義し、機密文書1001を構成することができる。データ変換部110はこのタグ付きデータと、ポリシー管理部109への許可・拒否の問い合わせにより提供可能なデータを再構成する。

【0027】ポリシー管理部109では、図11に示すマトリックスを用いて許可・拒否の判断を行なう。図11は、ユーザID301がuser Aの利用者はs1タグ501i付けされた社内秘データのみ閲覧可能、ユーザID301がuser Bの利用者はs3タグ501L付けされた役員データ以外は閲覧可能、ユーザID301がuser Cの利用者はすべてのデータが閲覧可能であることを示す。ここでデータ変換部110は、ユーザID301がuser Bである利用者に対してはs3タグで囲まれたデータを「****」マークに変換して閲覧不能にしている。変換されたHTMLファイルの例を図12に示す。データ変換部110から提供されたHTMLファイルは、先に述べたステップ210の暗号通信によりサービス利用者のアプリケーション実行部103に渡される。

【0028】この画面表示例を、図13に示す。ネットワーク上を流れるデータを第三者が盗聴した場合でも、暗号通信に用いる暗号鍵を復号化するための秘密鍵がなければ、図10の画面の表示を防止することが可能になる。

8

【0029】本実施の形態では、利用者が変わったり利用システムの状態が変わると、提供する情報も変化するところに特徴があり、機密保護、プライバシー保護を実現している。

【0030】次に、サービス利用部101が利用システム111に対して安全に操作を行なう方法について図14の処理フローを用いて説明する。例として図8においてポンプ停止ボタン805を押すことによって、ポンプ停止コマンドをサービス提供部104に送信する場合を考える。

【0031】ポンプ停止ボタン805が押された場合、サービス提供部104とサービス利用部101で同期をとっている値とコマンドのセットを、一つのデータとしてアプリケーション実行部103は作成する（ステップ1401）。同期を取っているデータとしては時刻やカウンタなどが考えられる。

【0032】図15に示すようにコマンド1501は、タグ付きデータとする。コマンドであることはcommandタグ501mで示され、targetタグ501nがコマンドの送信先、pumpタグ501aおよびstopタグ501cにより、ポンプを停止するコマンドであることを示す。「ad% f38wh! f74」は、利用システム111に対して実際に送信されるべき制御信号1502で、利用システム111に依存する特別な値である。

【0033】次に、タグ付きデータとしてのコマンド1501はユーザID301とカウンタ1503とともに、無作為に生成した暗号鍵を用いて暗号化され（ステップ1402）、暗号データ1504を形成する。暗号鍵はサービス提供部の公開鍵で暗号化する（ステップ1403）。暗号データ1504および暗号化された暗号鍵1505は、サービス利用部101の秘密鍵で署名される（ステップ1404）。アプリケーション実行部103では、暗号データ1504、暗号化された暗号鍵1505、署名データ1506、署名を検証するための電子証明書1507をセットにして基本認証部106に送信する（ステップ1405）。

【0034】基本認証部106では、電子証明書1507を検証してユーザの公開鍵を取得し（ステップ1406）、署名データ1503を公開鍵で検証する（ステップ1407）。基本認証部106はサービス提供部104の秘密鍵を用いて暗号化された暗号鍵1505を復号化し、暗号鍵を得る（ステップ1408）。この暗号鍵を用いて暗号データ1504を復号化し、カウンタ1503とコマンド1501を得る（ステップ1409）。基本認証部106はカウンタ1503を利用履歴管理部105に問い合わせ、既受信済みのものでないかどうかチェックする（ステップ1410）。受信済みであれば、コマンド1501を拒否し（ステップ1411）、受信済みでなければ、利用履歴管理部105に登録され

9

ている該ユーザのカウンタ1503を最新のものに更新し(ステップ1412)、コマンド1501をコマンド解析部に渡す(ステップ1413)。例えば、アプリケーション実行部103に保存されているユーザのカウンタ1503がnであった場合、カウンタ1503の値をn+1として添付する。送信されたカウンタ1503がn以下の場合には、送信データは既に受信済みであると判断して却下する。送信されたカウンタ1503がn+1であればコマンド1501を認証し、利用履歴管理部105の登録値をn+1に更新する。新規のカウンタ1503は、ユーザの公開鍵で暗号化されサービス利用部101に返信される(ステップ1414)。アプリケーション実行部103では、暗号化されたカウンタ1503を受信した場合に送達確認画面を表示し(ステップ1415)、ユーザの秘密鍵でカウンタ1503が復号化され、次のコマンド送信のために保存される(ステップ1416)。

【0035】本実施の形態では、サービス利用部101とサービス提供部104で同期している値を用いて同じコマンドの複数回の受信を防止しているところに特徴がある。インターネットを使ったシステムの場合、ネットワークの途中で盗聴したデータをそのまま送信する再送攻撃という不正アクセス技術があり、これを防止する。

【0036】また、誤って複数回ボタンを押してしまった場合にも、同じコマンドを複数受領することがなく、誤操作を防止することができる。また送信したコマンドが確実に利用システム111に送られたことも確認することができる。

【0037】コマンド解析部108における処理フローを図16に示す。コマンド解析部108は、コマンド1501のタグ501を解析し(ステップ1601)、ポリシー管理部109にタグ501の利用許可を問い合わせる(ステップ1602)。ポリシー管理部109ではユーザID301とタグ501、および利用システム111の状態に基づき許可・拒否の判断を行なう(ステップ1603)。拒否の場合には拒否である旨ユーザに通知し(ステップ1604)、許可の場合にはタグで囲まれた制御信号1502を利用システム111に送信する(ステップ1605)。

【0038】本実施の形態では、制御信号1502をタグ501で囲んで送信することによって、制御対象(例えばポンプ)の機器毎にデータフォーマットが異なる場合(例えばA社はX方式、B社はY方式など)にも、制御対象自体が同じであれば同じ方式によってアクセス制御が行なえるところに特徴がある。

【0039】

【発明の効果】以上述べたように、本発明によれば、利用者や利用システムの状態によって提供するコンテンツ自体を変化させ、機密保護、プライバシー保護を実現することができる。また、再送攻撃、誤操作を防止するこ

10

とができる。また、制御対象の機器毎にデータフォーマットが異なる場合にも、制御対象を同じタグで特徴付けることで同じ方式によってアクセス制御が適用可能であるところに特徴がある。

【図面の簡単な説明】

【図1】本発明を適用したサービス提供システムの全体構成図である。

【図2】本発明を適用したサービス利用者への情報提供処理の手続きを示すフローチャートである。

【図3】サービス利用部が利用者に対して提供する初期画面例である。

【図4】要求データ作成部において作成されるデータセットを示す図である。

【図5】データ格納部において格納されているプラント監視制御画面データの形式を示す図である。

【図6】ポリシー管理部において管理されているサービス提供を許可するか拒否するかを判断するルールを記述するマトリックスを示す図である。

【図7】データ変換部において変換されたプラント監視制御画面データの形式を示す図である。

【図8】データ変換部から渡されたプラント監視制御画面データを表示した画面例である。

【図9】ポリシー管理部において制限がかけられた場合の、データ変換部から渡されたデータを表示した画面例である。

【図10】データ格納部において格納されている機密データの形式を示す図である。

【図11】機密情報をどのユーザに許可するか拒否するかを判断するルールを記述するマトリックスを示す図である。

【図12】データ変換部において変換された機密データの形式を示す図である。

【図13】データ変換部から渡された機密データを表示した画面例である。

【図14】サービス利用部からサービス提供部にコマンドを送信する処理の手続きを示すフローチャートである。

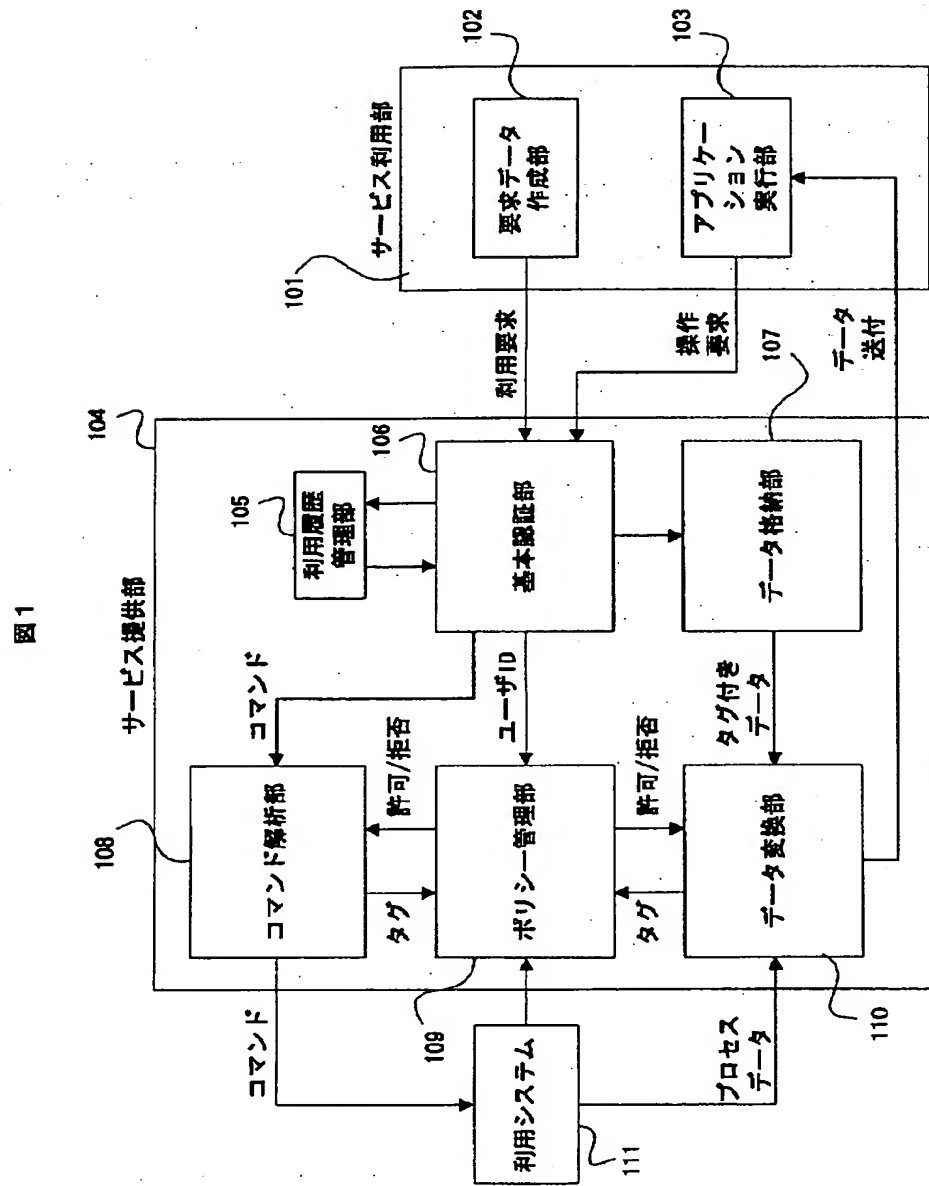
【図15】サービス利用部からサービス提供部に送られるデータセットの模式図である。

【図16】コマンド解析部における処理の手続きを示すフローチャートである。

【符号の説明】

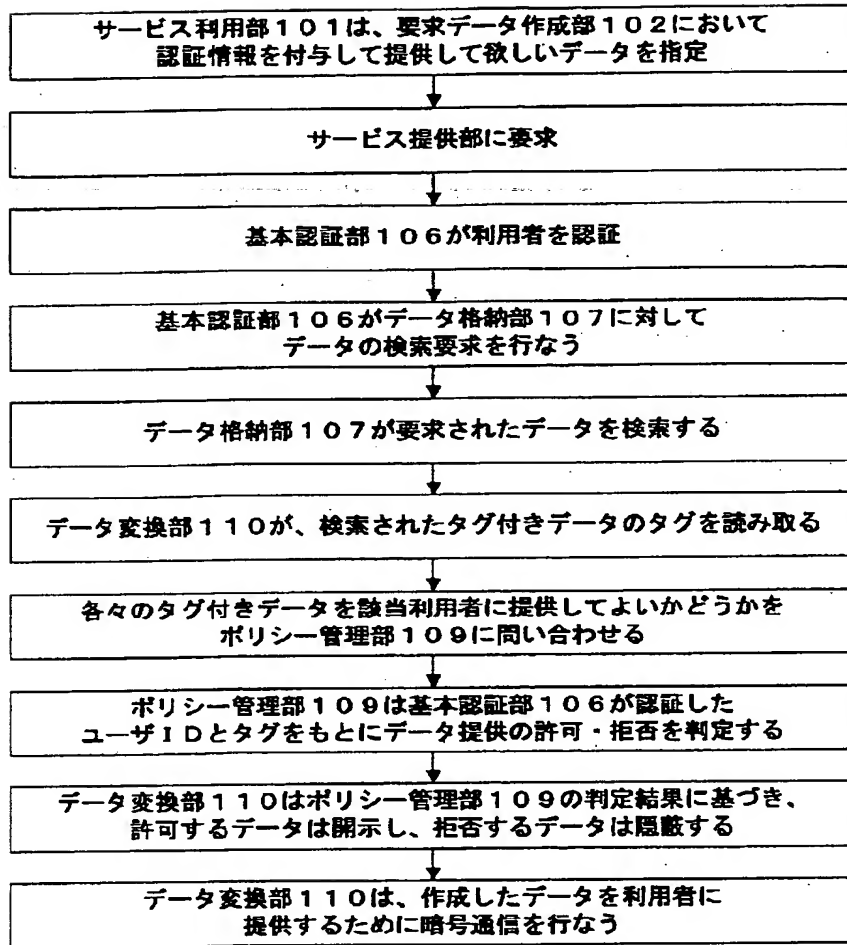
301…ユーザID、302…パスワード、304…要求データ、305…ログインボタン、306…キャンセルボタン、501…タグ、502…画面構成プログラム、601…条件文、701…変換されたファイル、801…ポンプ監視画面、802…ポンプ停止画面、803…バルブ監視画面、804…バルブ閉画面、805…ポンプ停止ボタン、1501…コマンド、1502…制御信号、1503…カウンタ、1504…暗号データ

【図1】



【図2】

図2



【図3】

図3

URL: <http://example/login/>

ユーザID:

パスワード:

利用希望サービス: ☐ ポンプ ☐ バルブ ☐ (他) 文書閲覧

【図12】

図12

```

<HTML>
<BODY>
  本契約における取引はA社とB社
  間で行われ、契約金は***であっ
  た。
</BODY>
</HTML>
  
```

【図4】

ユーザID:

デジタル署名:

証明書:

【図13】

URL: <https://example/secret/>

本契約における取引はA社とB社間で行われ、契約金は***であった。

【図5】

図5

```

<?XML Version=1.0?>
<PUMP>
  <WATCH pump_watch.class</WATCH>
  <START pump_start.class</START>
  <STOP pump_stop.class</STOP>
</PUMP>
<VALVE>
  <WATCH valve_watch.class</WATCH>
  <OPEN valve_start.class</OPEN>
  <CLOSE valve_stop.class</CLOSE>
</VALVE>
  
```

【図7】

図7

```

<HTML>
<BODY>
  <APPLET pump_watch.class</APPLET>
  <APPLET pump_start.class</APPLET>
  <APPLET pump_stop.class</APPLET>
  <APPLET valve_watch.class</APPLET>
  <APPLET valve_start.class</APPLET>
  <APPLET valve_stop.class</APPLET>
</BODY>
</HTML>
  
```

【図10】

図10

```

<?XML Version=1.0?>
<SECRET>
  本契約における取引は<a1>A社</a1>と
  <a2>B社</a2>間で行われ、契約金は
  <a3>3,000億円</a3>であった。
</SECRET>
  
```

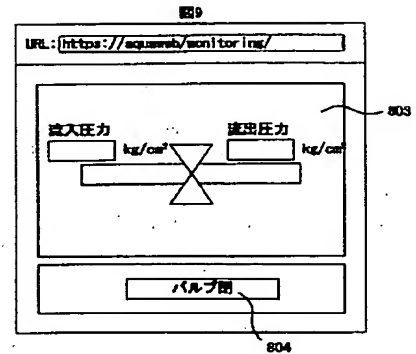
【図6】

図6

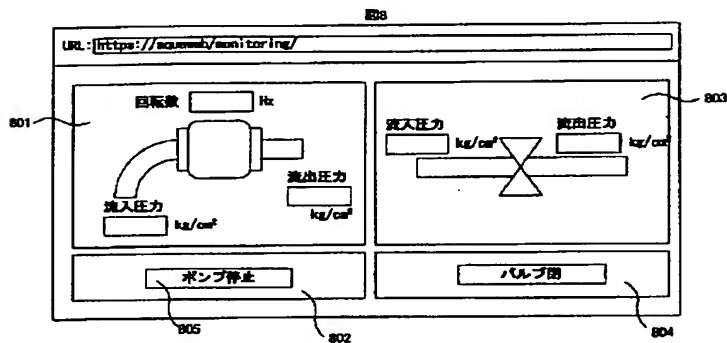
ユーザID	ポンプ pump			バルブ valves		
	監視 <watch>	起動 <start>	停止 <stop>	監視 <watch>	開 <open>	閉 <close>
userA ~ 301a	○	IF 1 > 8:00 and 1 < 17:00	×	○	×	×
userB ~ 301b	IF 電源 = on	×	IF 回転数 < 10000	○	×	○
userC ~ 301c	○	○	○	○	○	○

501b 501a 501c 501d 501f 501g 501h
601a 601b 601c

【図9】



【図8】



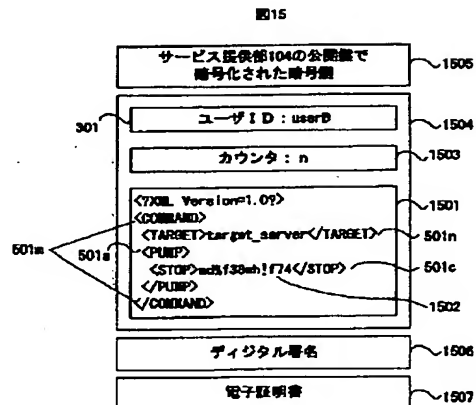
【図11】

図11

ユーザID	文書種類 (secret)			
	社外部 <s1>	幹部 <s2>	役員 <s3>	
userA ~ 301a	○	×	×	
userB ~ 301b	○	○	×	
userC ~ 301c	○	○	○	

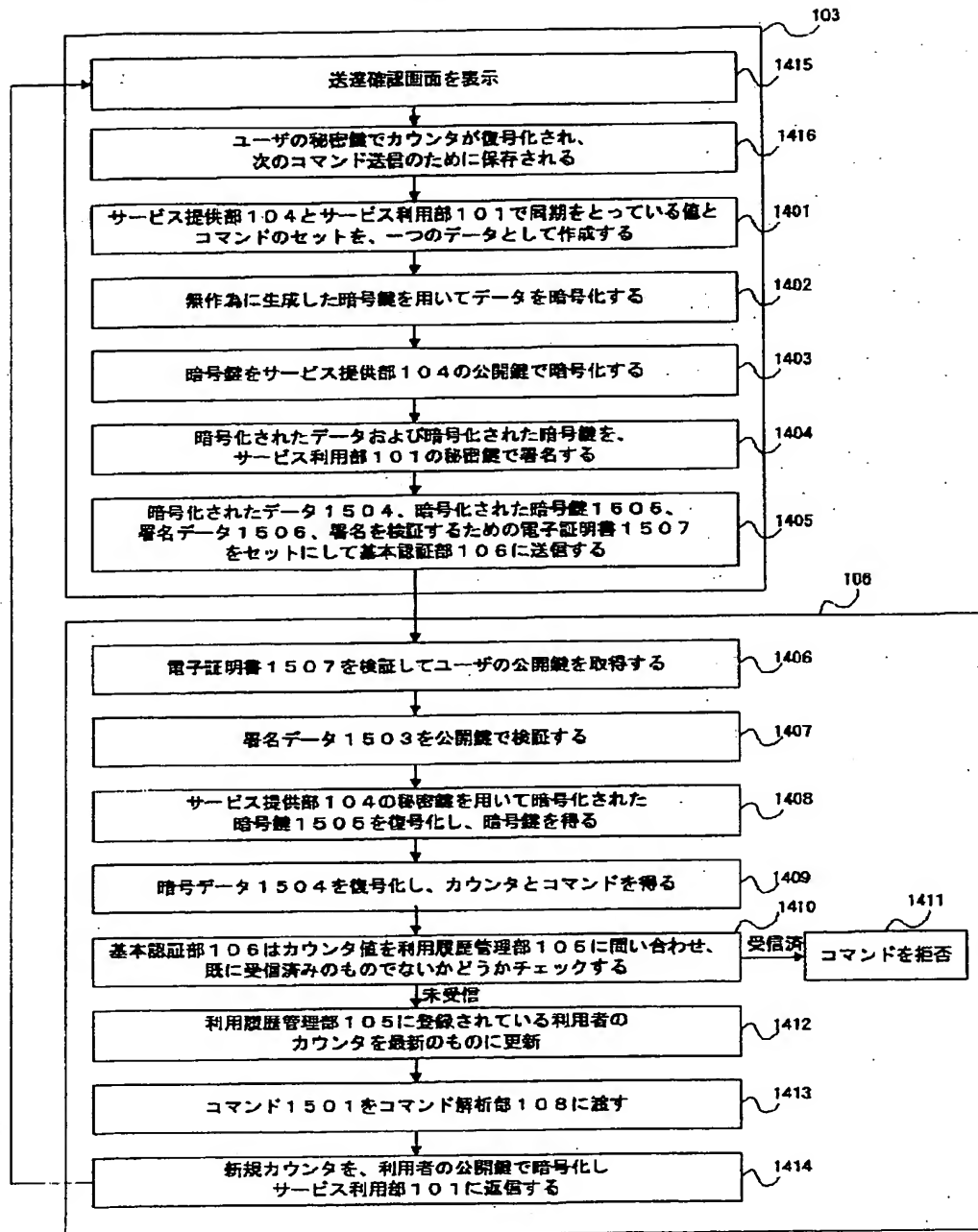
501j 501l 501k 501n

【図15】



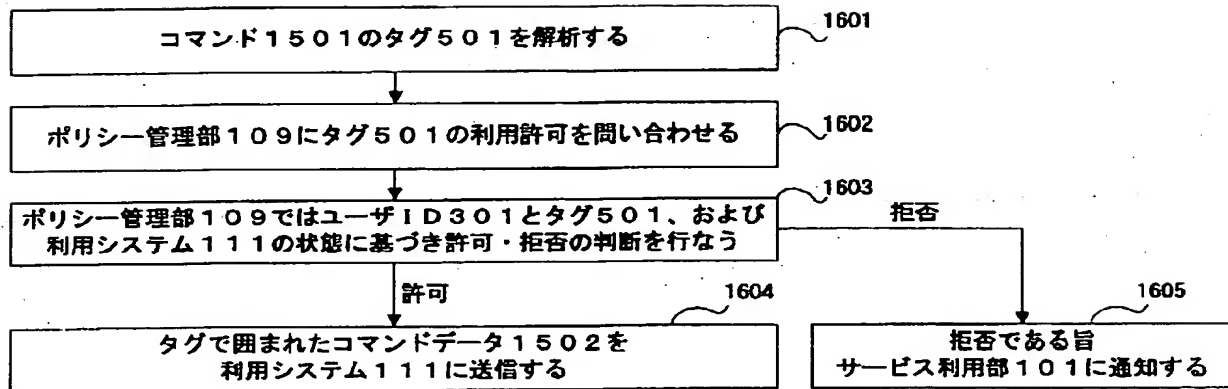
【図14】

図14



【図16】

図16



フロントページの続き

(51) Int. Cl. ⁷	識別記号	F I	テマコード (参考)
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 B
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 C
9/32			6 7 3 A

(72) 発明者 瀬古沢 照治
 神奈川県川崎市麻生区王禅寺1099番地 株
 式会社日立製作所システム開発研究所内 30

(72) 発明者 宮尾 健
 茨城県日立市大みか町五丁目2番1号 株
 式会社日立製作所情報制御システム事業部
 内
 Fターム (参考) 5B075 KK54 KK63 P002
 5B085 AE06 AE23 BE07
 5J104 AA07 AA09 AA16 EA05 EA06
 EA19 KA01 LA03 LA06 MA02
 NA02 NA05